

UNITED STATES DISTRICT COURT
for the
Northern District of Texas

In the Matter of the Search of
 (Briefly describe the property to be searched
 or identify the person by name and address)
 820 Sequoia Way
 Saginaw, Texas 76131

)
)
)
 Case No. 4:16-mj-377

Clerk, U.S. Dist. Ct. Court

By _____ Deputy

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment "A"

located in the Northern District of Texas, there is now concealed (identify the person or describe the property to be seized):

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

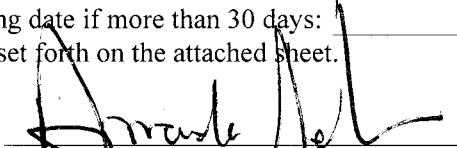
The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. §§ 2252 and 2252A	Posession and Receipt on Child Pornography

The application is based on these facts:

See Attached Affidavit

- Continued on the attached sheet.
- Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

Amanda Johnson, Special Agent, HSI

Printed name and title


Judge's signature

United States Magistrate Judge Jeffrey L. Cureton

Printed name and title

Sworn to before me and signed in my presence.

Date: 6/17/16

City and state: Fort Worth, Texas

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Special Agent, Amanda Johnson, of the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), being duly sworn under oath, do hereby depose and state:

1. I am a Special Agent with the United States Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), assigned to the Special Agent in Charge, Dallas, Texas. I have been employed with HSI since November 2007. As part of my duties as an HSI agent, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production and possession of child pornography, in violation of 18 U.S.C. §§ 2251, 2252, and 2252A. I have received training in the area of child pornography and child exploitation, and have had the opportunity to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous child pornography investigations and am very familiar with the tactics used by child pornography offenders who collect and distribute child pornographic material.

2. As a federal agent, I am authorized to investigate violations of the law of the United States and to execute warrants issued under the authority of the United States.

3. This affidavit is being made in support of an application for a search warrant for the residence located at **820 Sequoia Way, Saginaw, Texas**, for the items specified in Attachment B hereto.

4. The statements in this Affidavit are based in part on my investigation of this matter and on information provided by other law enforcement agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 18 U.S.C. §§, 2252, and 2252A, is located within the account identified in Attachment A.

5. The purpose of this application is to seize evidence, more particularly described in Attachment B, of violations of 18 U.S.C. §§ 2252 and 2252A, which make it a crime to possess, receive, or distribute child pornography.

DEFINITIONS

6. The following definitions apply to this Affidavit and Attachment B to this Affidavit:

7. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct,

or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

8. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

9. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

10. "Internet Service Providers" or "ISPs" are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial-up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e-mail address, and an e-mail mailbox, and the subscriber typically creates a password for the account.

By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

11. "Electronic Mail," commonly referred to as e-mail (or e-mail), is a method of exchanging digital messages from an author to one or more recipients. Modern e-mail operates across the Internet or other computer networks. E-mail systems are based on a store-and-forward model: e-mail servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need only connect briefly, typically to an e-mail server, for as long as it takes to send or receive messages. An Internet e-mail message generally consists of three components, the message envelope, the message header, and the message body, but may include a fourth component, an attachment. E-mail attachments can include any type of digital file. There are numerous methods of obtaining an e-mail account; some of these include e-mail accounts issued by an employer or school. One of the most common methods of obtaining an e-mail account is through a free web-based e-mail provider such as, MSN, Yahoo, or Gmail. Anyone that has access to the Internet can generally obtain a free web-based e-mail account.

12. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to,

phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

**BACKGROUND REGARDING THE
INTERNET/COMPUTERS AND CHILD PORNOGRAPHY**

13. I have been formally trained in the investigation of crimes involving the online sexual exploitation of children and have been investigating these crimes since 2008. Based on this training and knowledge, and the experience of other law enforcement personnel involved in this investigation, I know the following:

14. The Internet is a worldwide computer network that connects computers and allows communications and the transfer of data and information across state and national boundaries. A user accesses the Internet from a computer network or Internet Service Provider (“ISP”) that connects to the Internet. The ISP assigns each user an Internet Protocol (“IP”) Address. Each IP address is unique. Every computer or device on the Internet is referenced by a unique IP address the same way every telephone has a unique telephone number. An IP address is a series of four numbers separated by a period, and each number is a whole number between 0 and 255. An example of an IP address is 192.168.10.102.

Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP's customers or subscribers. Most ISP's employ dynamic IP addressing; that is, they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records, depending on the ISP's record retention policies.

15. Child pornographers can now transfer photographs from a camera or smartphone onto a computer-readable format with a device known as a scanner. With advent of digital cameras, the images can now be transferred directly onto a computer. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and distribute it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP) to anyone with access to a computer and modem.

Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

16. The computer's capability to store images in digital form makes it an ideal repository for child pornography. A single floppy or compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 250 gigabytes are not uncommon. These drives can store thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

17. With Internet access, a computer user can transport an image file from the Internet or from another user's computer to his own computer, so that the image file is stored in his computer. The process of transporting an image file to one's own computer is called "downloading." The user can then display the image file on his computer screen, and can choose to "save" the image on his computer and/or print out a hard copy of the image by using a printer device (such as a laser or inkjet printer).

18. Importantly, computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little to no cost. Even when such files have been deleted, they may be recoverable months or years later using readily-available forensic tools. When a person “deletes” a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or cache. The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

BACKGROUND OF INVESTIGATION – WEBSITE “A”

19. Since at least June 2012, the Homeland Security Investigations (HSI), Child Exploitation Investigations Unit (CEIU), as well as various international law enforcement agencies, has been investigating an online website that has been used extensively by

persons interested in exchanging images depicting child pornography to meet and become trading partners. This website is hereinafter referred to as "Website A."

20. Website A is a photo-sharing (still image) website, hosted outside of the United States. Membership is free and includes unlimited hosting storage and free photo sharing of digital images. Website A is organized by different sections according to topic, such as "architecture," "travel," "family," and "auto." Within each section are albums that are both created and named by Website A members.

21. To become a "member" of Website A, a user must register to obtain an account. The user must supply a username and provide a valid e-mail address in order to receive a password provided by Website A. Upon receiving this password, the user is prompted to create a new password which will be used to log in to Website A. Once this is done, the user, as a member, may create albums and post images within these sections. A user's albums are listed under his/her username. A member can create one or more photo albums and has the option of making an album available to all individuals on the Web (a "public album") or password protecting the album so that it is only accessible to individuals who know or have the password. When a member creates an album he/she may choose to have his/her contact e-mail address displayed under his/her username (which appears at the top of the album), or he/she can ask others to "contact via comments." Even in instances where a member does not display his/her e-mail address under his/her username, it is not uncommon for the member to post the email address in the comment section as a means of contact or in response to a specific request from another member.

22. An album consists of all the pictures associated with that album, along with any posted comments. When a member creates an album, he/she has a choice via a scroll down menu to disable the comment feature or allow comments from (1) only Website A members who have created albums on Website A; (2) only registered Website A members (regardless of whether they have created their own albums on Website A); or (3) anyone accessing Website A (whether or not they are a Website A member), who may anonymously comment on the album.

23. Anytime an individual posts a comment to an album, the owner of that album is automatically notified by Website A via the e-mail he/she provided as his/her contact e-mail address. The e-mail message states that a comment was made, and includes the file name of the image commented on, the comment itself, the user name of the person making the comment (if the person posting the comment is a Website A member) and a hyperlinked URL to the image with the corresponding comment. While the member who is the owner of an album cannot directly opt out of receiving these e-mail notifications, if he/she were to go back to his/her membership profile and delete the e-mail address, he/she would not receive these automated e-mail notifications.

24. Any individual on the Internet can view and post comments (based on how the owner of the album set up the comments) to non-password protected albums ("public albums") on Website A and download images from those albums. Only members can create albums and upload pictures to them. When a member posts a comment to an album, that member's username, a country flag corresponding to the originating IP address, and the date and time of the comment are displayed next to the comment.

When a comment is posted by a non-member of Website A, portions of the originating IP address and a country flag corresponding to that IP address are displayed next to that comment. Regardless of whether the individual posting a comment is a member or non-member, Website A logs the full originating IP address of the individual posting the comment.¹

25. Website A has become a popular means for individuals to trade child pornography images, in particular through the “nudity” and “kids” sections. Examples of the names of albums within these two sections are “Boys: Pure summer camp fun,” “webscams cute little boys” and “Todler/kids Potty time.” Some Website A albums associated with some of the targets of national and international investigations are known to contain child pornography. In these cases, the child pornography is most likely to be in a password-protected album, rather than in a public album. While most of the images law enforcement has seen posted in public albums may not constitute child pornography, often evidence from the images, and comments posted about the album (either by other individuals or the member who created the album), indicate that the particular poster or person who created the album has a sexual interest in children and that these individuals’ interest in Website A lies in the ability to meet other individuals for the private trading of child pornography. A common scenario is for such a user to post child erotica or preview pictures of children, accompanied by a sexually suggestive title or comment, in a public album as a way to entice or attract other individuals with a sexual interest in children.

¹ The HSI Cyber Crimes Center, Child Exploitation Investigations Unit (CEIU) is not currently receiving user logs containing IP addresses from foreign law enforcement, although logs have been received in the past.

The poster's purpose is often to solicit comments on the pictures posted from like-minded individuals. Once these individuals meet on Website A, they then agree to trade Website A passwords, or trade their private child pornography collections elsewhere, often by e-mail, rather than risking trading child pornography on Website A itself. Individuals on the Internet, including Website A users, may regularly monitor public albums on Website A and post provocative comments or images in specific albums related to children with the hope of obtaining the password to other password protected albums or information on individuals that are willing to trade child pornography.

26. I have been informed that The High Technology Investigative Unit located within the U.S. Department of Justice's Child Exploitation and Obscenity Section has been involved in the investigation of more than two dozen Website A users who either posted sexually explicit images of children to Website A or distributed sexually explicit images of children to another user to obtain their password. In more than half of these cases, investigation revealed that these individuals were actively molesting children and in some instances posting images of that abuse to Website A. I have also conducted federal investigations within north Texas involving individuals who posted child erotica and sexually explicit images of children to Website A and were found to be actively molesting children.

INVESTIGATION RELATED TO OLDMANYG

27. On or about May 21, 2016, an undercover Police Officer with the Queensland Police Service (Brisbane, Queensland, Australia) reviewed the user account “OLDMANYG” in the Kids section of Website A and identified three photo albums labeled as “Cute butts,” “Bikinis” and “9 y/o school girls” associated with the account. The album titled “9 y/o school girls” was password protected. The open album named “Cute butts” contained fourteen photos of prepubescent minor females wearing bathing suits; all of the photos were taken from behind, showcasing the back side of their body. Comments from OLDMANYG and other users indicate a sexual interest in the minors depicted in the photos. For example, on May 23, 2016, OLDMANYG posted the following comment to one of his photos depicting a close-up image of a minor female’s buttocks in a swimming suit: “want to kiss it.” On a separate photo depicting a minor female wearing a bathing suit and looking back toward the camera, OLDMANYG posted the comment: “love to look and dream.” The User Info for OLDMANYG stated “Beauty is beauty, inspires feelings that not acted on. Imagination is wonderful.” The account was registered on May 20, 2016.

28. The undercover officer posted a message to one of OLDMANYG’S photos and OLDMANYG responded from his e-mail account, identified as “fmya2x@gmail.com.” OLDMANYG and the undercover officer began exchanging e-mails about the sexual exploitation of children. OLDMANYG sent images of minor children in a classroom setting and explained to the undercover officer that he was a teacher and had taken the pictures of his students without their knowledge with his cellular phone.

One such e-mail reads:

“Never gone to camp with them, I am into being on the receiving end of BDSM, I fantasize about the girls finding me passed out and they decide to strip me and tie spread eagle from a tree branch. They find my toy stash and the pics I have taken of them so they decide to punish me. They force a ball gag in my mouth before I wake up. They find my collection of floggers and shock wands and start flogging me on all sides while others seem to delight in using the shock wands on my cock and balls. They me begging through my gag for them to stop. Finally they do and offer me a deal, they will strip naked and stay that way if I beg them to hurt me. They will stay naked as long as they are hurting me, once they stop they will get dressed my choice naked and take the punishment? Or freedom but no naked 9 year olds. I only pause for a moment before I started begging them to hurt me. Like my fantasy?”

OLDMANYG attached an image to this e-mail, filename 20160523_085112.jpg, which depicted a minor female sitting at a desk in a classroom. The minor is wearing black leggings with black boots and her legs are spread open. The focus of the camera is between the minor’s legs. The undercover officer recovered exif² data from the image, which indicated it was taken with a Samsung SM0G920A smartphone on May 23, 2016, at 8:47 AM, CST.

² EXIF is short for Exchangeable Image File, a format that is a standard for storing interchange information in digital photography image files using JPEG compression. Almost all new digital cameras use the EXIF annotation, storing information on the image such as shutter speed, exposure compensation, what metering system was used, if a flash was used, ISO number, date and time the image was taken and GPS information.

29. In an e-mail dated May 24, 2016, OLDMANYG advised the undercover officer that he once had nude images of children, but his hard drive crashed and he would have to spend time searching his back-up to locate them. The content of the e-mail is stated below:

“I do not have any naked of my grankids. Panties don't do any thing for me. It is the fantasy inenjoy. KNowing what emotions they evoke in other men turns me on. I am a bit of a mental voyer. I had some from the web, but hard drive crash took them. This summer I will have time to search my backup and see what I can recover.”

30. In addition to communicating with the undercover officer about his sexual fantasies with minors, OLDMANYG requested images of the undercover officer's step-daughter. In an e-mail dated May 22, 2016, OLDMANYG wrote: “I lost alot of photos because of a hard drive crash several years ago. Would like to hear more about your step daughter. Any pics? I am looking forward to the neighbor pool this summer. Cell phone cameras are great.” Also, in an e-mail dated May 23, 2016, OLDMANYG requests images of the undercover officer's step-daughter again and writes: “I am a teacher. I look only, comments don't offend me. I love to hear about others thoughts, the more graphic the better. Any pics of your step daughter?”

31. The undercover officer obtained IP logs from Website A regarding user OLDMANYG and determined the IP address associated with the account was 162.236.27.3, which is owned by Internet Service Provider AT&T; the IP address geolocates to the Fort Worth, Tarrant County, Texas area.

The undercover officer subsequently sent all corresponding information related to this investigation to the HSI Cyber Crimes Center (C3) for consideration. C3 subsequently forwarded the information to the HSI Dallas, Texas field office.

32. On May 25, 2016, I sent a DHS summons to AT&T for subscriber information related to IP address 162.236.27.3. AT&T responded to the summons and provided the following information:

Name: Mark Stutheit
Address: 820 Sequoia Way, Saginaw, Texas 76131
Phone: [redacted]-7038
IP Start Date: May 18, 2016
IP End Date: May 22, 2016

33. I conducted a search of the Texas Workforce Commission database and learned that Mark Stutheit is employed by the Dallas Independent School District. I conducted open source Internet searches and learned Stutheit is a fourth-grade teacher at an elementary school located in Dallas, Texas. I conducted a search in databases commonly used by law enforcement and determined Mark Stutheit resides at 820 Sequoia Way in Saginaw, Tarrant County, Texas, which is located within the Northern District of Texas, Fort Worth Division. A search of the Tarrant County Appraisal District revealed the property/residence at 820 Sequoia Way is owned by Mark Stutheit and [redacted] Stutheit.

34. On May 26, 2016, I conducted physical surveillance at 820 Sequoia Way and observed a Mercury Cougar bearing Texas license plates DJ7S997 parked on the street in front of the residence. I conducted checks and determined the vehicle was registered to Mark Stutheit, 820 Sequoia Way, Saginaw, Texas 76131.

CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

35. Based on my training and experience, and conversations with other law enforcement officials familiar with the traits and characteristics of child pornography collectors, I can attest that certain characteristics are generally found to exist in cases involving individuals who collect child pornography. These characteristics include the following:

- a. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage of their collections of illicit materials.
- b. The majority of individuals who collect child pornography often seek like-minded individuals, either in person or on the internet, to share information and trade depictions of child pornography as a means of gaining status, trust, acceptance and support. The different internet-based vehicles used by such individuals to communicate with each other include, but are not limited to: email, email groups, bulletin boards, forums, newsgroups, instant messaging, and other similar vehicles.
- c. The majority of individuals who collect child pornography often store identifying information concerning child victims, as well as identifying information about other individuals who share the same interests.
- d. Based on my training and experience, the suspect in this case appears to be a collector of child pornography. I base this opinion on the following:

- i. Mark Stutheit is employed in a position of trust as an educator at a DISD elementary school and used that position of trust to produce sexually suggestive images

of minors;

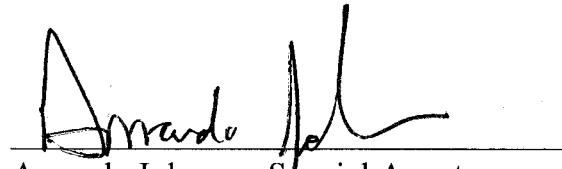
ii. The sexually suggestive images produced by Stutheit, among others, were posted on Website A, which is a vehicle known to law enforcement to meet like-minded individuals. Stutheit encouraged other members of Website A to comment on the images;

iii. Stutheit admitted to the undercover officer that he possessed nude images of minors and would attempt to recover them from a back-up of a hard drive that crashed. Although Stutheit indicated that the hard drive had crashed some years previously, his comments about attempting a recovery this summer suggest that he has retained this hard drive. Thus, in addition to this information supporting that Stutheit is a collector of child pornography, there is also probable cause to believe that he has child pornography images on a hard drive still in his possession.

iv. Stutheit admitted his sexual interest in children and requested sexually explicit images of the undercover officer's minor step-daughter.

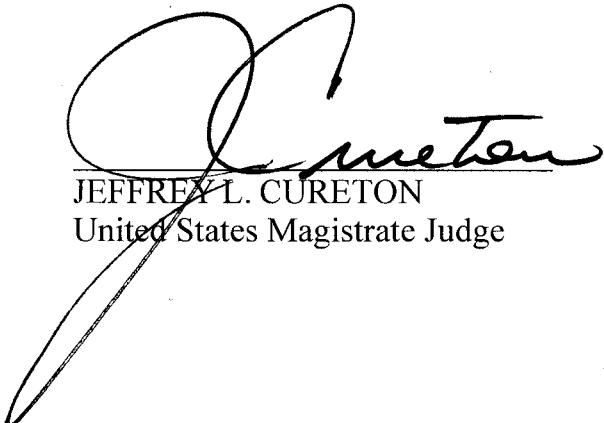
36. Based on the aforementioned factual information, there is probable cause to believe that evidence, fruits, and instrumentalities may be located at the address described in Attachment A, in violation of 18 U.S.C. §§ 2252 and 2252A. Rule 41 of the Federal Rules of Criminal Procedure authorizes the government to seize and retain evidence and instrumentalities of a crime for a reasonable time, and to examine, analyze, and test them.

37. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the location described in Attachment A and seizure of the items listed in Attachment B.



Amanda Johnson, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on June 17th, 2016, at 2:25 a.m./p.m. in Fort Worth, Texas.



JEFFREY L. CURETON
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF ITEM TO BE SEARCHED

820 Sequoia Way, Saginaw, Texas 76131

The residence is described as a 2,441 square foot, two-story residence, constructed of brown brick with beige trim. "820" is displayed on the brick next to the garage door. This residence is located in Saginaw, Tarrant County, which is within the Northern District of Texas.

The search also includes the search of vehicles located at or near the premises, which fall under the dominion and control of the person or persons associated with said premises. The search of these vehicles is to include all internal and external compartments and all containers that may be associated with the storage of child pornographic materials or their instrumentalities contained within the aforementioned vehicles.



ATTACHMENT B
DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

1. Computers, tablets, mobile devices/cellular phones to include a Samsung SM0G920A smartphone, hard drives and computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Evidence of who used, owned, or controlled the computer(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, accounts of Internet Service Providers.
3. Records evidencing occupancy or ownership of the premises described above, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence, rental or lease agreements, mortgage documents, rental or lease payments and credit card information, including, but not limited to, bills and payment records.

4. Any and all notes, documents, records, computer files or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the production, possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the production, possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

5. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

6. Any and all cameras, film, videotapes or other photographic equipment.